PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:		Confirmation No.:	2870
	Todd Fischer	Group Art Unit:	3621
Serial No.:	10/053,375	Examiner:	John W. Hayes
Filed:	10/25/01	Docket No.	10012680-1

For: **SECURE REMOTE PRINTING VIA A COMMUNICATION NETWORK**

Certificate of Mailing
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, postage prepaid, in an envelope addressed to: Mail Stop Appeal Brief; Commissioner for Patents, U.S. Patent & Trademark Office, P.O. Box 1450 Alexandria, Virginia 22313-1450, on
5/17/05.

Stephanie Riley
Signature –

APPEAL BRIEF UNDER 37 C.F.R. §41.37

Mail Stop Appeal Brief - Patents
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This is an appeal from the decision of Examiner John W. Hayes, Group Art Unit 3621, mailed March 4, 2005, rejecting claims 1, 2, 4 – 13 and 15 - 19 in the present application and making the rejection FINAL.

I. REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). H PDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF THE CLAIMS

Claims 1, 2, 4 – 13 and 15 – 19 remain pending.

IV. STATUS OF AMENDMENTS

Applicant submitted a response after final with amendments that amended claims 1, 5, 11 and 18. That response was entered. A copy of the current claims is attached hereto as Exhibit A.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The invention relates to secure printing systems and methods. In this regard, an embodiment of a secure printing system 10 (*see* FIG. 1 and page 4, line 19 – page 5, line 17, for example), such as recited in claim 1, comprises a printing device 130 (*see* FIG. 1 and page 5, lines 18 - 24, for example). The printing device 130 is configured to print information as hard copy. The printing device 130 has located therein a remote print system 100 (*see* FIG. 1 and page 5, line 6 – page 6, line 22, for example). In this embodiment, the remote printing system 100 is configured to: provide a user with an encryption key (*see* page 5, lines 8 – 10, for example); receive information encrypted using the encryption key (*see* page 5, lines 15 – 17, for example); decrypt the information with a corresponding decryption key (*see* page 5, lines 15 – 17, for example); and enable the information, once decrypted, to be printed (*see* page 5, lines 15 – 17, for example).

Another embodiment of a secure printing system 10 for printing information (*see* FIG. 1 and page 4, line 19 – page 5, line 17, for example), such as recited in claim 11, comprises a printing device 130 (*see* FIG. 1 and page 5, lines 18 - 24, for example). In this embodiment, the information is stored in memory at a location remote from a user, with the information being accessible to the user via a communication network 160 (*see* FIG. 1 and page 6, lines 9 - 19, for example). The printing device 130 is operative to print information as hard copy. The printing device also has contained therein a remote print system 100 (*see* FIG. 1 and page 5, line 6 – page 6, line 22, for example). In this embodiment, the remote print system is arranged at a location remote from the information and is configured to provide a user with an encryption key (*see* FIG. 4 and page 10, lines 13 – 24, for example). The remote print system 100 also is configured to communicate with the communication network 160 such that the remote print system receives information encrypted using the encryption key (*see* FIG. 4 and page 10, lines 21 – 25, for example). The remote print system 100 is further configured to decrypt the information with a corresponding decryption key (*see* FIG. 4 and page 10, line 25 – page 11, line 7, for example) and enable the information, once decrypted, to be printed (*see* FIG. 4 and page 11, lines 13 – 24, for example). Once the information is decrypted using the decryption key, the printing device 130 is enabled to print the information as hard copy (*see* page 5, lines 15 - 17, for example).

An embodiment of a method for secure printing of information transmitted via a communication network also is provided, such as recited in claim 15. In this embodiment, the information is stored in memory at a first location remote from a user, with the information being accessible to the user via the communication network. This method comprises: providing the user with an encryption key from a printing device (*see* FIG. 4 and page 10, lines 13 - 24, for example); receiving, at the printing device located at a second location remote from the first location, information encrypted using the encryption key via the communication network (*see* FIG. 4 and page 10, lines 21 - 25, for example); decrypting the information with a corresponding decryption key using the printing device (*see* FIG. 4 and page 10, line 25 - page 11, line 7, for example); and enabling the information, once decrypted, to be printed by the printing device (*see* FIG. 4 and page 11, lines 13 - 24, for example).

Another embodiment of a method for secure printing of information transmitted via a communication network is recited in claim 18. In this embodiment, the information is stored in memory at a first location remote from a user, the information being accessible to the user via the communication network. This method comprises: enabling an encryption key to be received from a printing device located at a second location remote from the first location (*see* FIG. 6 and page 12, lines 10 - 20, for example); enabling information that is to be printed to be identified (*see* FIG. 7 and page 10, line 21 - page 13, line 12, for example); and enabling the encryption key and information corresponding to the information that is to be printed to be transmitted to the first location via the communication network such that the information that is to be printed is encrypted using the encryption key (*see* FIG. 7 and page 13, lines 13 - 16, for example), transmitted to the printing device located at the second location via the communication network (*see* FIG. 6 and page 12, lines 16 - 20, for example), decrypted by the printing device using a corresponding decryption key (*see* FIG. 4 and page 10, line 25 - page 11, line 7, for example), and printed by the printing device (*see* FIG. 4 and page 11, lines 13 - 24, for example).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1 - 2, 6, 7, 11, 12, 15 and 18 stand finally rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Zingher* in view of *Maldy*.

Claims 4, 5, 13, 16, and 17 stand finally rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Zingher* and *Maldy* in view of *Chomet*.

Claims 8 - 10 stand finally rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Zingher* in view of *Maldy* and *Barkan*.

VII. ARGUMENT

A. Independent Claim 1 and Dependent Claims 2 and 4 - 10

The primary reference asserted against Applicant's independent claim 1 is *Zingher*. In this regard, *Zingher* generally involves a print job allocation system. As disclosed in *Zingher*, that reference teaches:

> Using a printing plants profile generated from the data received from the printing machines 22 via the printing machine control devices 24 and the print job requirements profile generated from the data received from the data input devices 32, the print job processor 14 determines which printing machine(s) 22 in which printing plant(s) 20 are capable and available for processing a print job of the type input by the printing plant customer 30. Here, it is particularly important that the distribution requirements of the printed product, included in the requirements profile, are simultaneously

> taken into account when determining the optimum use of the printing machines 22 located throughout the world. Thus, as early as during the allocation of the print job for later dispatching of the print job, the distribution requirements of a print job are considered.
>
> In the print job processor 14, the job requests entered by the customers 30 via the network 12 are compared against the free or available capacity input to the print job processor 14 via the printing machine control devices 24 of each of the printing plants 20. A particular print job is allocated and distributed to one or more printing plants 20 in accordance with the requirements profile generated from the data input by the customers 30 via the data input devices 32. As a result, each print job can be carried out in the best possible manner with regard to the optimization of time, material costs, desired quality and any other suitable criteria.

(*Zingher*, col. 5, line 60 to col. 6, line 18).

Applicant respectfully asserts that, as shown in the exemplary teaching of *Zingher* above, *Zingher's* printing device is not involved with decryption of information that is to be printed.

Additionally, *Zingher* discloses:

> ***The data transmitted over the network 12 can be encrypted using known encryption devices and authentication codes***, as desired, for security of data and to prevent tampering with print job requests or printing plant data. All of the data transmitted in the print job allocation system 10 may be encrypted for maximum security. Alternatively, various selected data transmissions in the print job allocation system 10 may be encrypted as desired. For example, it may be desirable to encrypt only data relating to print job requests and transmit the printing plant data in an unencrypted format.

(*Zingher*, col. 3, lines 41 - 51). (Emphasis Added).

Applicant also respectfully notes that *Zingher* has only disclosed using "known encryption devices and authentication codes," for performing encryption. Since the only teaching of record of the use of a printing device for decrypting information is that found in Applicant's disclosure, Applicant respectfully asserts that *Zingher* may not be properly asserted as teaching or reasonably suggesting at least this feature. This is in direct contrast to Applicant's claimed systems and methods as will be described in detail.

Additionally, the Office Action makes what appears to be general comments pertaining to Applicant's disclosure and then seems to use these general comments as the basis for the pending rejections. In particular, the final Office Action states:

> The Applicant's Disclosure states that the remote print system is preferably implemented by or otherwise associated with a printing device and can be implemented in software, firmware, hardware, or a combination thereof (Specification, page 6, lines 20 – 22). In the printing device software implementation, Applicant describes a system analogous to the teachings of Zingher ('260, figure 2) where the remote printing system is a computer implemented as or associated with a printing device (Specification, page 7, lines 4 - 7).
>
> Therefore the Examiner maintains the rejection to Applicant's claims.

(Final Office Action, page 2, line 14 – page 3, line 5).

Applicant respectfully asserts that even if portions of Applicant's disclosure were proven to be known and, therefore, unpatentable (unless in patentable combination with other features), it is the features recited in the pending claims that are to be compared to the prior art. That is, it is improper to compare Applicant's disclosure to the prior art without regard to the claimed invention. In this regard, Applicant is entitled to disclose more than that which is claimed. Thus, since there is adequate support for the features recited in the pending claims, the specific features of the claims must be shown unpatentable irrespective of what other material may be present in Applicant's disclosure.

In this regard, claim 1 recites:

> 1. A secure printing system comprising:
> ***a printing device configured to print information as hard copy, the printer having located therein a remote print system*** configured to:
> provide a user with an encryption key,
> receive information encrypted using the encryption key,
> ***decrypt the information with a corresponding decryption key***, and
> enable the information, once decrypted, to be printed.

(Emphasis Added).

Applicant respectfully asserts that the cited art, either individually or in combination, is legally deficient for the purpose of rendering claim 1 unpatentable. In particular, Applicant respectfully asserts that none of the references or combinations thereof teaches or reasonably suggests at least the features/limitations emphasized above in claim 1. That is, Applicant respectfully asserts that none of the other cited references teaches or reasonably suggests the features/limitations described above as lacking in *Zingher*. Thus, Applicant respectfully asserts that the pending rejections are legally deficient for rendering the claim 1 obvious under 35 U.S.C. § 103. Therefore, Applicant respectfully asserts that claim 1 is in condition for allowance.

Since claims 2 and 4 - 10 are dependent claims that incorporate all the features/limitations of claim 1, Applicant respectfully asserts that these claims also are in condition for allowance. Additionally, these claims recite other features/limitations that can serve as an independent basis for patentability.

B. Independent Claim 11 and Dependent Claims 12 and 13

The primary reference asserted against Applicant's independent claim 11 is *Zingher*. In this regard, *Zingher* generally involves a print job allocation system. As disclosed in *Zingher*, that reference teaches:

> Using a printing plants profile generated from the data received from the printing machines 22 via the printing machine control devices 24 and the print job requirements profile generated from the data received from the data input devices 32, the print job processor 14 determines which printing machine(s) 22 in which printing plant(s) 20 are capable and available for processing a print job of the type input by the printing plant customer 30. Here, it is particularly important that the distribution requirements of the printed product, included in the requirements profile, are simultaneously taken into account when determining the optimum use of the printing machines 22 located throughout the world. Thus, as early as during the allocation of the print job for later dispatching of the print job, the distribution requirements of a print job are considered.
>
> In the print job processor 14, the job requests entered by the customers 30 via the network 12 are compared against the free or available capacity input to the print job processor 14 via the printing machine control

> devices 24 of each of the printing plants 20. A particular print job is allocated and distributed to one or more printing plants 20 in accordance with the requirements profile generated from the data input by the customers 30 via the data input devices 32. As a result, each print job can be carried out in the best possible manner with regard to the optimization of time, material costs, desired quality and any other suitable criteria.

(*Zingher*, col. 5, line 60 to col. 6, line 18).

Applicant respectfully asserts that, as shown in the exemplary teaching of *Zingher* above, *Zingher's* printing device is not involved with decryption of information that is to be printed.

Additionally, *Zingher* discloses:

> ***The data transmitted over the network 12 can be encrypted using known encryption devices and authentication codes***, as desired, for security of data and to prevent tampering with print job requests or printing plant data. All of the data transmitted in the print job allocation system 10 may be encrypted for maximum security. Alternatively, various selected data transmissions in the print job allocation system 10 may be encrypted as desired. For example, it may be desirable to encrypt only data relating to print job requests and transmit the printing plant data in an unencrypted format.

(*Zingher*, col. 3, lines 41 - 51). (Emphasis Added).

Applicant also respectfully notes that *Zingher* has only disclosed using "known encryption devices and authentication codes," for performing encryption. Since the only teaching of record of the use of a printing device for decrypting information is that found in Applicant's disclosure, Applicant respectfully asserts that *Zingher* may not be properly asserted as teaching or reasonably suggesting at least this feature. This is in direct contrast to Applicant's claimed systems and methods as will be described in detail.

Additionally, the Office Action makes what appears to be general comments pertaining to Applicant's disclosure and then seems to use these general comments as the basis for the pending rejections. In particular, the final Office Action states:

> The Applicant's Disclosure states that the remote print system is preferably implemented by or otherwise associated with a printing device and can be implemented in software, firmware, hardware, or a combination thereof (Specification, page 6, lines 20 – 22). In the printing device software

> implementation, Applicant describes a system analogous to the teachings of Zingher ('260, figure 2) where the remote printing system is a computer implemented as or associated with a printing device (Specification, page 7, lines 4 - 7). Therefore the Examiner maintains the rejection to Applicant's claims.

(Final Office Action, page 2, line 14 – page 3, line 5).

Applicant respectfully asserts that even if portions of Applicant's disclosure were proven to be known and, therefore, unpatentable (unless in patentable combination with other features), it is the features recited in the pending claims that are to be compared to the prior art. That is, it is improper to compare Applicant's disclosure to the prior art without regard to the claimed invention. In this regard, Applicant is entitled to disclose more than that which is claimed. Thus, since there is adequate support for the features recited in the pending claims, the specific features of the claims must be shown unpatentable irrespective of what other material may be present in Applicant's disclosure.

In this regard, claim 11 recites:

> 11. A secure printing system for printing information, the information being stored in memory at a location remote from a user, the information being accessible to the user via a communication network, said secure printing system comprising:
>
> a printing device operative to print information as hard copy, ***the printing device having contained therein a remote print system, the remote print system being arranged at a location remote from the information and configured to provide a user with an encryption key***,
>
> said remote print system being configured to communicate with the communication network such that said remote print system receives information encrypted using said encryption key,
>
> ***said remote print system being further configured to decrypt said information with a corresponding decryption key, and enable said information, once decrypted, to be printed***;
>
> wherein once said information is decrypted using said decryption key, said printing device is enabled to print said information as hard copy.

(Emphasis Added).

Applicant respectfully asserts that the cited art, either individually or in combination, is legally deficient for the purpose of rendering claim 11 unpatentable. In particular, Applicant respectfully asserts that none of the references or combinations thereof teaches or reasonably suggests at least the features/limitations emphasized above in claim 11. That is, Applicant respectfully asserts that none of the other cited references teaches or reasonably suggests the features/limitations described above as lacking in *Zingher*. Thus, Applicant respectfully asserts that the pending rejections are legally deficient for rendering the claim 11 obvious under 35 U.S.C. § 103. Therefore, Applicant respectfully asserts that claim 11 is in condition for allowance.

Since claims 12 and 13 are dependent claims that incorporate all the features/limitations of claim 11, Applicant respectfully asserts that these claims also are in condition for allowance. Additionally, these claims recite other features/limitations that can serve as an independent basis for patentability.

C. Independent Claim 15 and Dependent Claims 16 and 17

The primary reference asserted against Applicant's independent claim 15 is *Zingher*. In this regard, *Zingher* generally involves a print job allocation system. As disclosed in *Zingher*, that reference teaches:

> Using a printing plants profile generated from the data received from the printing machines 22 via the printing machine control devices 24 and the print job requirements profile generated from the data received from the data input devices 32, the print job processor 14 determines which printing machine(s) 22 in which printing plant(s) 20 are capable and available for processing a print job of the type input by the printing plant customer 30. Here, it is particularly important that the distribution requirements of the printed product, included in the requirements profile, are simultaneously taken into account when determining the optimum use of the printing machines 22 located throughout the world. Thus, as early as during the allocation of the print job for later dispatching of the print job, the distribution requirements of a print job are considered.
>
> In the print job processor 14, the job requests entered by the customers 30 via the network 12 are compared against the free or available capacity input to the print job processor 14 via the printing machine control

> devices 24 of each of the printing plants 20. A particular print job is allocated and distributed to one or more printing plants 20 in accordance with the requirements profile generated from the data input by the customers 30 via the data input devices 32. As a result, each print job can be carried out in the best possible manner with regard to the optimization of time, material costs, desired quality and any other suitable criteria.

(*Zingher*, col. 5, line 60 to col. 6, line 18).

Applicant respectfully asserts that, as shown in the exemplary teaching of *Zingher* above, *Zingher's* printing device is not involved with decryption of information that is to be printed.

Additionally, *Zingher* discloses:

> ***The data transmitted over the network 12 can be encrypted using known encryption devices and authentication codes***, as desired, for security of data and to prevent tampering with print job requests or printing plant data. All of the data transmitted in the print job allocation system 10 may be encrypted for maximum security. Alternatively, various selected data transmissions in the print job allocation system 10 may be encrypted as desired. For example, it may be desirable to encrypt only data relating to print job requests and transmit the printing plant data in an unencrypted format.

(*Zingher*, col. 3, lines 41 - 51). (Emphasis Added).

Applicant also respectfully notes that *Zingher* has only disclosed using "known encryption devices and authentication codes," for performing encryption. Since the only teaching of record of the use of a printing device for decrypting information is that found in Applicant's disclosure, Applicant respectfully asserts that *Zingher* may not be properly asserted as teaching or reasonably suggesting at least this feature. This is in direct contrast to Applicant's claimed systems and methods as will be described in detail.

Additionally, the Office Action makes what appears to be general comments pertaining to Applicant's disclosure and then seems to use these general comments as the basis for the pending rejections. In particular, the final Office Action states:

> The Applicant's Disclosure states that the remote print system is preferably implemented by or otherwise associated with a printing device and can be implemented in software, firmware, hardware, or a combination thereof (Specification, page 6, lines 20 – 22). In the printing device software

> implementation, Applicant describes a system analogous to the teachings of Zingher ('260, figure 2) where the remote printing system is a computer implemented as or associated with a printing device (Specification, page 7, lines 4 - 7). Therefore the Examiner maintains the rejection to Applicant's claims.

(Final Office Action, page 2, line 14 – page 3, line 5).

Applicant respectfully asserts that even if portions of Applicant's disclosure were proven to be known and, therefore, unpatentable (unless in patentable combination with other features), it is the features recited in the pending claims that are to be compared to the prior art. That is, it is improper to compare Applicant's disclosure to the prior art without regard to the claimed invention. In this regard, Applicant is entitled to disclose more than that which is claimed. Thus, since there is adequate support for the features recited in the pending claims, the specific features of the claims must be shown unpatentable irrespective of what other material may be present in Applicant's disclosure.

In this regard, claim 15 recites:

> 15. A method for secure printing of information transmitted via a communication network, the information being stored in memory at a first location remote from a user, the information being accessible to the user via the communication network, said method comprising:
>
> ***providing the user with an encryption key from a printing device***;
>
> receiving, at the printing device located at a second location remote from the first location, information encrypted using the encryption key via the communication network;
>
> ***decrypting the information with a corresponding decryption key using the printing device***; and
>
> enabling the information, once decrypted, to be printed by the printing device.

(Emphasis Added).

Applicant respectfully asserts that the cited art, either individually or in combination, is legally deficient for the purpose of rendering claim 15 unpatentable. In particular, Applicant respectfully asserts that none of the references or combinations thereof teaches or reasonably suggests at least the features/limitations emphasized above in claim 15. That is, Applicant respectfully asserts that none of the other cited references teaches or reasonably suggests the features/limitations described above as lacking in *Zingher*. Thus, Applicant respectfully asserts that the pending rejections are legally deficient for rendering the claim 15 obvious under 35 U.S.C. § 103. Therefore, Applicant respectfully asserts that claim 15 is in condition for allowance.

Since claims 16 and 17 are dependent claims that incorporate all the features/limitations of claim 15, Applicant respectfully asserts that these claims also are in condition for allowance. Additionally, these claims recite other features/limitations that can serve as an independent basis for patentability.

D. Independent Claim 18

The primary reference asserted against Applicant's independent claim 18 is *Zingher*. In this regard, *Zingher* generally involves a print job allocation system. As disclosed in *Zingher*, that reference teaches:

> Using a printing plants profile generated from the data received from the printing machines 22 via the printing machine control devices 24 and the print job requirements profile generated from the data received from the data input devices 32, the print job processor 14 determines which printing machine(s) 22 in which printing plant(s) 20 are capable and available for processing a print job of the type input by the printing plant customer 30. Here, it is particularly important that the distribution requirements of the printed product, included in the requirements profile, are simultaneously taken into account when determining the optimum use of the printing machines 22 located throughout the world. Thus, as early as during the allocation of the print job for later dispatching of the print job, the distribution requirements of a print job are considered.
>
> In the print job processor 14, the job requests entered by the customers 30 via the network 12 are compared against the free or available capacity input to the print job processor 14 via the printing machine control devices 24 of each of the printing plants 20. A particular print job is allocated and distributed to one or more printing plants 20 in accordance with the requirements profile generated from the data input by the customers 30 via the data input devices 32. As a result, each print job can be carried out in the best possible manner with regard to the optimization of time, material costs, desired quality and any other suitable criteria.

(*Zingher*, col. 5, line 60 to col. 6, line 18).

Applicant respectfully asserts that, as shown in the exemplary teaching of *Zingher* above, *Zingher's* printing device is not involved with decryption of information that is to be printed.

Additionally, *Zingher* discloses:

> ***The data transmitted over the network 12 can be encrypted using known encryption devices and authentication codes***, as desired, for security of data and to prevent tampering with print job requests or printing plant data. All of the data transmitted in the print job allocation system 10 may be encrypted for maximum security. Alternatively, various selected data transmissions in the print job allocation system 10 may be encrypted as desired. For example, it may be desirable to encrypt only data relating to print job requests and transmit the printing plant data in an unencrypted format.

(*Zingher*, col. 3, lines 41 - 51). (Emphasis Added).

Applicant also respectfully notes that *Zingher* has only disclosed using "known encryption devices and authentication codes," for performing encryption. Since the only teaching of record of the use of a printing device for decrypting information is that found in Applicant's disclosure, Applicant respectfully asserts that *Zingher* may not be properly asserted as teaching or reasonably suggesting at least this feature. This is in direct contrast to Applicant's claimed systems and methods as will be described in detail.

Additionally, the Office Action makes what appears to be general comments pertaining to Applicant's disclosure and then seems to use these general comments as the basis for the pending rejections. In particular, the final Office Action states:

> The Applicant's Disclosure states that the remote print system is preferably implemented by or otherwise associated with a printing device and can be implemented in software, firmware, hardware, or a combination thereof (Specification, page 6, lines 20 – 22). In the printing device software implementation, Applicant describes a system analogous to the teachings of Zingher ('260, figure 2) where the remote printing system is a computer implemented as or associated with a printing device (Specification, page 7, lines 4 - 7). Therefore the Examiner maintains the rejection to Applicant's claims.

(Final Office Action, page 2, line 14 – page 3, line 5).

Applicant respectfully asserts that even if portions of Applicant's disclosure were proven to be known and, therefore, unpatentable (unless in patentable combination with other features), it is the features recited in the pending claims that are to be compared to the prior art. That is, it is improper to compare Applicant's disclosure to the prior art without regard to the claimed invention. In this regard, Applicant is entitled to disclose more than that which is claimed. Thus, since there is adequate support for the features recited in the pending claims, the specific features of the claims must be shown unpatentable irrespective of what other material may be present in Applicant's disclosure.

In this regard, claim 18 recites:

> 18. A method for secure printing of information transmitted via a communication network, the information being stored in memory at a first location remote from a user, the information being accessible to the user via the communication network, said method comprising:
>
> ***enabling an encryption key to be received from a printing device*** located at a second location remote from the first location;
>
> enabling information that is to be printed to be identified; and
>
> enabling the encryption key and information corresponding to the information that is to be printed to be transmitted to the first location via the communication network ***such that the information that is to be printed is encrypted using the encryption key, transmitted to the printing device located at the second location via the communication network, decrypted by the printing device using a corresponding decryption key, and printed by the printing device.***

(Emphasis Added).

Applicant respectfully asserts that the cited art, either individually or in combination, is legally deficient for the purpose of rendering claim 18 unpatentable. In particular, Applicant respectfully asserts that none of the references or combinations thereof teaches or reasonably suggests at least the features/limitations emphasized above in claim 18. That is, Applicant respectfully asserts that none of the other cited references teaches or reasonably suggests the features/limitations described above as lacking in *Zingher*. Thus, Applicant respectfully asserts that the pending rejections are legally deficient for rendering the claim 18 obvious under 35

U.S.C. § 103. Therefore, Applicant respectfully asserts that claim 18 is in condition for allowance.

CONCLUSION

Based upon the foregoing discussion, Applicant respectfully requests that the Examiner's final rejection of the pending claims be overruled and withdrawn by the Board, and that the application be allowed to issue with all pending claims.

Please charge Hewlett-Packard Company's deposit account 08-2025 in the amount of $340 for the filing of this Appeal Brief. No additional fees are believed to be due in connection with this Appeal Brief. If, however, any additional fees are deemed to be payable, you are hereby authorized to charge any such fees to deposit account No. 08-2025.

Respectfully submitted,

M. Paul Qualey, Jr., Reg. 43,024

(770) 933-9500

VIII. CLAIMS - APPENDIX

1. (Previously Presented) A secure printing system comprising:

a printing device configured to print information as hard copy, the printer having located therein a remote print system configured to:

provide a user with an encryption key,

receive information encrypted using the encryption key,

decrypt the information with a corresponding decryption key, and

enable the information, once decrypted, to be printed.

2. (Original) The secure printing system of claim 1, wherein said remote print system generates the encryption key and the corresponding decryption key.

3. (Canceled)

4. (Previously Presented) The secure printing system of claim 1, wherein said printing device includes a display device; and

wherein the encryption key is displayed to the user via the display device.

5. (Previously Presented) The secure printing system of claim 1, wherein the remote print system has an address usable for providing information to the remote print system via a communication network; and

wherein the remote print system is configured to provide the user with the address.

6. (Original) The secure printing system of claim 1, further comprising:

a data retrieval/encryption system arranged at a location remote from the remote print system, the data retrieval/encryption system being configured to communicate with the remote print system via a communication network, the data retrieval/encryption system being further configured to receive the encryption key and information corresponding to information that the user intends to print such that the data retrieval/encryption system locates the information that the user intends to print, encrypts the information that the user intends to print using the encryption key, and communicates the information in an encrypted form to the remote print system.

7. (Original) The secure printing system of claim 6, wherein the data retrieval/encryption system is configured to communicate to the user, via the communication network, that information is available for printing such that, if the user desires the information to be printed, the user can obtain an encryption key from the remote print system and communicate the encryption key to the data retrieval/encryption system for use in encrypting the information to be printed.

8. (Previously Presented) The secure printing system of claim 6, further comprising:

a print request system communicating with the data retrieval/encryption system, the print request system being configured to receive the encryption key and information corresponding to information that the user intends to print such that the print request system communicates the encryption key and the information corresponding to information that the user intends to print to the data retrieval/encryption system.

9. (Original) The secure printing system of claim 8, wherein the print request system is implemented by a portable computing device.

10. (Original) The secure printing system of claim 9, wherein the portable computing device communicates with the data retrieval/encryption system via wireless communication.

11. (Previously Presented) A secure printing system for printing information, the information being stored in memory at a location remote from a user, the information being accessible to the user via a communication network, said secure printing system comprising:

a printing device operative to print information as hard copy, the printing device having contained therein a remote print system, the remote print system being arranged at a location remote from the information and configured to provide a user with an encryption key,

said remote print system being configured to communicate with the communication network such that said remote print system receives information encrypted using said encryption key,

said remote print system being further configured to decrypt said information with a corresponding decryption key, and enable said information, once decrypted, to be printed;

wherein once said information is decrypted using said decryption key, said printing device is enabled to print said information as hard copy.

12. (Original) The secure printing system of claim 11, further comprising:

means for providing the user with said encryption key.

13. (Original) The secure printing system of claim 12, wherein said means for providing the user with said encryption key is a display device.

14. (Canceled)

15. (Previously Presented) A method for secure printing of information transmitted via a communication network, the information being stored in memory at a first location remote from a user, the information being accessible to the user via the communication network, said method comprising:

providing the user with an encryption key from a printing device;

receiving, at the printing device located at a second location remote from the first location, information encrypted using the encryption key via the communication network;

decrypting the information with a corresponding decryption key using the printing device; and

enabling the information, once decrypted, to be printed by the printing device.

16. (Previously Presented) The method of claim 15, further comprising:

providing the user with an address usable for providing information to the printing device located at the second location via the communication network.

17. (Original) The method of claim 15, wherein the encryption key is provided to the user visually.

18. (Previously Presented) A method for secure printing of information transmitted via a communication network, the information being stored in memory at a first location remote from a user, the information being accessible to the user via the communication network, said method comprising:

enabling an encryption key to be received from a printing device located at a second location remote from the first location;

enabling information that is to be printed to be identified; and

enabling the encryption key and information corresponding to the information that is to be printed to be transmitted to the first location via the communication network such that the information that is to be printed is encrypted using the encryption key, transmitted to the printing device located at the second location via the communication network, decrypted by the printing device using a corresponding decryption key, and printed by the printing device.

19. (Original) The method of claim 18, wherein enabling the encryption key and information corresponding to the information that is to be printed to be transmitted comprises:

enabling the encryption key and information corresponding to the information that is to be printed to be transmitted via wireless communication.

20. (Canceled)

IX. EVIDENCE - APPENDIX

None.

IX. RELATED PROCEEDINGS- APPENDIX

None.